DENSE RANDOM FINITELY GENERATED SUBGROUPS OF LIE GROUPS

JÖRG WINKELMANN

1. The result

The purpose of this paper is to prove the following theorem:

Theorem. *Let G be a connected real Lie group of dimension n.*

Then there exists a relatively compact open neighbourhood W of e in G such that for $n+1$ randomly chosen elements $g_0, \ldots, g_n$ the generated subgroup will be dense in G with probability one.

2. Preparations

2.1. **The probability measure.** Every locally compact group admits a "Haar measure" which is finite iff the group is compact.[1] The measure of a compact subset is always finite, the measure of an open subset always non-zero. Therefore, by renormalizing we obtain an induced probability measure for every relatively compact open subset.

In other words, if, given a Lie group G and a relatively compact open subset $W \subset G$, we say "$k+1$ randomly chosen elements $g_0, \ldots, g_k$ in W have the property X with probability one", then this means the following:

Let

$$\Sigma = \{(g_0, \ldots, g_k) \in W^{k+1} : (g_0, \ldots, g_k) \text{ has property } X\}.$$

Let μ be a Haar measure on G and μ^{k+1} the induced product measure on G^{k+1}. Then $\mu^{k+1}(\Sigma) = \mu^{k+1}(W^{k+1})$.

2.2. **Zassenhaus neighbourhoods.** Inspired by the classical notion of a *Zassenhaus neighborhood* we introduce:

Acknowledgement. The author wants to thank the organizers of "Groups and Probability", L. Pyber and M. Abért, for the invitation to participate in this conference and E. Breuillard for asking the question which is answered by this article.

[1] Here it does not matter whether we consider left- or rightinvariant Haar measures.

Definition 1. *Let G be a connected real Lie group. For an element $g \in G$ let $\zeta_g : G \to G$ be the commutator map, i.e., $\zeta_g(h) = ghg^{-1}h^{-1}$.*

A Z-neighbourhood W is an open relatively compact subset of G such that $e \in W$ and $\lim_{k\to\infty}(\zeta_g)^k(x) = e$ for all $g, x \in W$.

Developing the group law on G into a power series, it becomes obvious that every real Lie group admits a Z-neighbourhood.

We use this definition rather than the classical notion of a Zassenhaus neighborhood[2] because for our definition it is clear that it is stable under taking quotients of Lie groups:

Fact 1. *Let $\phi : G \to H$ be a surjective homomorphism of real Lie groups and W a Z-neighbourhood in G.*

Then $\phi(W)$ is a Z-neighbourhood in H.

2.3. **Regular elements.** We recall the notions of Cartan subalgebras and regular elements in Lie groups. As standard references we use [1], [3] and [4].

Definition 2. *Let $\mathbf{g}$ be a finite-dimensional Lie algebra over a field k. A Lie subalgebra $\mathbf{h}$ is called* Cartan subalgebra *if it is nilpotent and equals its own normalizer (i.e. $[x, a] \in \mathbf{h}\ \forall a \in \mathbf{h}$ implies $x \in \mathbf{h}$.)*

Definition 3. *Let G be a Lie group. An element $g \in G$ is called* regular *if the multiplicity of 1 as root of the characteristic polynomial of $Ad(g)$ is minimal.*

This definition implies immediately that the set of all non regular elements in a connected Lie group constitutes a nowhere dense real analytic subset. In particular (see e.g. [7] for more details):

Fact 2. *Let G be a connected real Lie group and G_{reg} the subset of all regular elements.*

Then $G \setminus G_{reg}$ has Haar measure zero.

Lemma 1. *Let G be a connected real Lie group, g a regular element and H a connected closed normal subgroup of G which contains g.*

Then G/H is nilpotent.

Proof. For a complex number λ let V_λ be the associated weight space for $Ad(g)$, i.e.

$$V_\lambda = \left\{ v \in (Lie\, G) \otimes_{\mathbb{R}} \mathbb{C} : (Ad(g) - \lambda I)^N (v) = 0\ \exists N > 0 \right\}.$$

[2] Classically, a neighbourhood U of e in G is called a *Zassenhaus neighbourhood* iff every discrete subgroup of G generated by its intersection with U must be nilpotent.

Then evidently $V_\lambda \subset (Lie\, H) \otimes_{\mathbb{R}} \mathbb{C}$ for all $\lambda \neq 0$. Therefore V_0 surjects onto $(Lie\, G/ Lie\, H) \otimes_{\mathbb{R}} \mathbb{C}$. But for a regular element g the weight space V_0 is a Cartan subalgebra of $Lie\, G$ and therefore a nilpotent Lie subalgebra of $Lie\, G$. Hence G/H must be nilpotent. □

2.4. **The commutative case.**

Lemma 2. *Let H be a subgroup of $G = (\mathbb{R}^n, +)$.*

Then either H is dense in G or there exists a surjective $\mathbb{R}$-linear map $F : \mathbb{R}^n \to \mathbb{R}$ with $F(H) \subset \mathbb{Z}$.

Proof. Let $\bar{H}$ be the closure of H in G. The quotient $G/\bar{H}$ is a commutative connected real Lie group and therefore isomorphic to some $(S^1)^d \times \mathbb{R}^g$. Both $\mathbb{R}$ and S^1 admit surjective Lie group homomorphisms onto S^1. Thus either H is dense in G or there is a surjective Lie group homomorphism from $G/\bar{H} \to S^1$. Using the isomorphism $S^1 \simeq \mathbb{R}/\mathbb{Z}$ it is clear that in the latter case there is a surjective $\mathbb{R}$-linear map F from $\mathbb{R}^n$ to $\mathbb{R}$ with $F(H) \subset \mathbb{Z}$. □

Lemma 3. *Let $G = \mathbb{R}^n$. Then there is a set Σ of Haar (i.e. Lebesgue) measure zero in G^{n+1} such that for every $(g_1, \ldots, g_{n+1}) \in G^{n+1} \setminus \Sigma$ the subgroup of G generated by the g_i is dense.*

Proof. Let Σ_0 denote the set of all $(g_1, \ldots, g_{n+1})$ for which G is not generated as a $\mathbb{R}$-vector space by $g_1, \ldots, g_n$. For each $(g_1, \ldots, g_{n+1}) \notin \Sigma_0$ the element g_{n+1} can be expressed as $\mathbb{R}$-linear combination of the other g_i:

$$g_{n+1} = \sum_{j=1}^{n} a_j g_j \quad \exists a_j \in \mathbb{R} \tag{1}$$

We define $\Sigma_1 \subset G^n \setminus \Sigma_0$ as the set of all $(g_1, \ldots, g_{n+1})$ such that the real numbers $1, a_1, \ldots, a_n$ are not $\mathbb{Q}$-linearly independent.

We set $\Sigma = \Sigma_0 \cup \Sigma_1$. Let $(g_1, \ldots, g_{n+1}) \in G^{n+1} \setminus \Sigma$. Let $(a_j)_{1 \leq j \leq n}$ as in eq. 1. Then (due to the definition of Σ) the real numbers $1, a_1, \ldots, a_n$ are $\mathbb{Q}$-linearly independent. As a consequence we obtain:

$$\sum_j a_j b_j \notin \mathbb{Q}$$

for any choice of $b_1, \ldots, b_n \in \mathbb{R}$ unless all the b_j are zero.

This implies: If $F : \mathbb{R}^n \to \mathbb{R}$ is a non-zero $\mathbb{R}$-linear map with $F(g_1), \ldots, F(g_n) \in \mathbb{Q}$, then $F(g_{n+1}) \notin \mathbb{Q}$.

Therefore there does not exist a non-zero $\mathbb{R}$-linear map $F : G \to \mathbb{R}$ with $F(\Gamma) \subset \mathbb{Q}$ and a forteriori no such map with $F(\Gamma) \subset \mathbb{Z}$. By lemma 2 it thus follows that Γ is dense in G whenever $(g_1, \ldots, g_{n+1}) \notin \Sigma$. □

2.5. **The nilpotent case.** We recall the notion of the (descending) central series:

Given a group G and subsets $A, B \subset G$ let $[A, B]$ denote the set of all commutators $aba^{-1}b^{-1}$ with $a \in A$ and $b \in B$.

The groups $G^{[k]}$ of the central series are defined recursively: $G^1 = G$ and if $G^{[k]}$ is already defined, one defines $G^{[k+1]}$ as the closure of the subgroup of G generated by the elements of $[G, G^{[k]}]$.

A group G is nilpotent iff there exists a number $n \in \mathbb{N}$ such that $G^{[n]} = \{e\}$.

By definition $G^{[2]}$ coincides with the *commutator group* G'.

Lemma 4. *Let G be a real nilpotent Lie group and H a subgroup. Assume that $HG^{[2]}$ is dense in G.*

Then H is dense in G.

Proof. We start the proof of the lemma by claiming that $H^{[k]}G^{[k+1]}$ is dense in $G^{[k]}$ for all $k \in \mathbb{N}$. We will show this claim by induction on k. Thus let us assume that $H^{[k]}G^{[k+1]}$ is dense in $G^{[k]}$. We have to show that under this assumption $H^{[k+1]}G^{[k+2]}$ must be dense in $G^{[k+1]}$. Now $G^{[k+1]}$ is topologically generated by $[G, G^{[k]}]$. Since $HG^{[2]}$ is dense in G and $H^{[k]}G^{[k+1]}$ is dense in $G^{[k]}$, it follows that the image of $[H, H^{[k]}]$ must be dense in $[G, G^{[k]}]/A$ where A is topologically generated by $[G^{[2]}, G^{[k]}]$ and $[G, G^{[k+1]}]$. Since $[G^{[2]}, G^{[k]}]$ and $[G, G^{[k+1]}]$ are both contained in $G^{[k+2]}$, it follows that $H^{[k+1]}G^{[k+2]}$ is dense in $G^{[k+1]}$. This proves the claim.

Next we show by induction in the opposite direction that $H^{[k]}$ is dense $G^{[k]}$ for all $k \in \mathbb{N}$. For k sufficiently large this is trivially true since $H^{[k]} = G^{[k]} = \{e\}$ for all sufficiently large k. Now let us assume that $H^{[k]}$ is dense in $G^{[k]}$. Then $H^{[k-1]} = H^{[k-1]} \cdot H^{[k]}$ is dense in $H^{[k-1]} \cdot G^{[k]}$ which in turn is dense in $G^{[k-1]}$. Thus we deduce by (descending) induction on k that $H^{[k]}$ is dense in $G^{[k]}$ for all $k \in \mathbb{N}$. In particular, $H = H^{[1]}$ is dense in $G = G^{[1]}$. □

Proposition 1. *Let G be a connected nilpotent real Lie group, and $d = \dim(G/G')$.*

Then there exists a subset $\Sigma \subset G^{d+1}$ of Haar measure zero such that for every $(g_0, \ldots, g_d) \in G^{d+1} \setminus \Sigma$ the subgroup of G generated by the g_i is dense in G.

Proof. Let $\tau : G \to G/G'$ be the natural projection. Thanks to lemma 3 we know that there is a subset $\Sigma_0 \subset (G/G')^{d+1}$ of Haar measure zero such that $d+1$ elements $g_0, \ldots, g_d \in G/G'$ generate a dense subgroup unless $(g_0, \ldots, g_d) \in \Sigma_0$.

Let $\Sigma = \tau^{-1}(\Sigma_0)$. Then Σ has Haar measure zero and for each $(g_0, \ldots, g_d) \in G^{d+1} \setminus \Sigma$ the generated subgroup Γ has a dense image in G/G'.

Finally due to lemma 4 the condition $\overline{\tau(\Gamma)} = G/G'$ implies $\overline{\Gamma} = G$. □

3. Proof of the main result

Proposition 2. *Let G be a connected real Lie group of dimension n, W a Z-neighbourhood and $0 \le k \le n$.*

Let $g_0, \ldots, g_k \in W$ be randomly chosen elements and H_k the closure of the subgroup of G generated by $g_0, \ldots, g_k$.

Then with probability one at least one of the following two conditions is fulfilled:

- *There is a normal closed Lie subgroup M in G with $M \subset H_k$ such that G/M is nilpotent.*
- $\dim H_k \ge k$.

Proof. The proof works by induction on k. For $k = 0$ there is nothing to prove.

Thus let us assume $k > 0$ and let us furthermore assume that H^0_{k-1} has the desired property. In other words, we assume that

$$(g_0, \ldots, g_{k-1}) \in W$$

are given such that the closure H_{k-1} of the group generated by these elements has the desired property and we want to show that under this assumption a randomly chosen element $g_k \in W$ has with probability one the property that $g_0, \ldots, g_{k-1}$ and g_k together generate a subgroup with the desired property.

Since the set of non-regular elements of G is a set of Haar measure zero (fact 2), we may and do assume that all the g_i are regular elements.

If H^0_{k-1} contains a closed subgroup M such that H^0_{k-1} and G/M nilpotent, so does H^0_k and we are done. Therefore we may assume that H^0_{k-1} satisfies the second property, i.e. $\dim H_{k-1} \ge k-1$.

We distinguish three cases:

(1) H^0_{k-1} is not normal in G.
(2) H^0_{k-1} is normal and $g_0 \notin H^0_{k-1}$.
(3) H^0_{k-1} is normal and $g_0 \in H^0_{k-1}$.

In the first case the normalizer of H^0_{k-1} in G is a proper real Lie subgroup of G, implying that with probability one $g_k H^0_{k-1} g_k^{-1}$ is not contained in H^0_{k-1} for a randomly chosen $g_k \in W$. But then H^0_{k-1} and

$g_k H^0_{k-1} g_k^{-1}$ generate a Lie subgroup I with $\dim(I) > \dim(H_{k-1}) \geq k-1$ and $I \subset H_k$. Hence $\dim H_k \geq k$ with probability one in this case.

In the second case let us consider the projection $\pi : G \to A = G/H^0_{k-1}$. Note that $\pi(W)$ is a Z-neighbourhood in A (see fact 1). We are done if A is nilpotent. Thus we may and do assume that A is not nilpotent. Since we are in the second case, $\pi(g_0) \in \pi(W) \setminus \{e_A\}$. Recall that we assumed g_0 to be a regular element in G. Thus the Lie subalgebra of $Lie\, G$ defined by the zero weight space of $Ad(g_0)$ is a Cartan subalgebra and in particular it is nilpotent. Since A is not nilpotent, this Cartan subalgebra can not map surjectively on A. Therefore there is a non-zero complex number λ which occurs as eigen value for $Ad(\pi(g_0)) \in GL(Lie\, A)$. As a consequence $\zeta^N_{\pi(g_0)} : A \to A$ is never a constant map (here $\zeta_{\pi(g_0)}$ is the commutator map, i.e. $\zeta_{\pi(g)}(h) = ghg^{-1}h^{-1}$.) Thus $\zeta^N_{\pi(g_0)}(\pi(g_k)) \neq e$ with probability one for all $N \in \mathbb{N}$ and a randomly chosen element $g_k \in W$. On the other hand $\lim_{N\to\infty} \zeta^N_{\pi(g_0)}(\pi(g)) = e$ for all $g \in W$, because $\pi(W)$ is a Z-neighbourhood in A. It follows that with probability one the subgroup of A generated by $\pi(g_0)$ and $\pi(g_k)$ is not discrete. This implies $\dim(H_k) > \dim(H_{k-1})$ and thereby $\dim(H_k) \geq k$.

It remains to discuss the third case. However, since g_0 is regular, the assumptions "H^0_{k-1} is normal in G and $g_0 \in H^0_{k-1}$" do imply that G/H^0_{k-1} is nilpotent (see lemma 1). Thus we found a connected Lie subgroup M with G/M nilpotent and $M \subset H_k$, namely $M = H^0_{k-1}$. □

Corollary 1. *Let G be a real connected Lie group of dimension n and W a Z-neighbourhood.*

For randomly chosen elements $g_0, \ldots, g_n \in W$ let H be the closure of the subgroup generated by the g_i.

Then with probability one there exists a normal closed Lie subgroup M of G such that G/M is nilpotent and $M \subset H$.

Proof. By prop. 2 with $k = n$ we know that there is such a Lie subgroup M unless $\dim(H) \geq n$. But $\dim(H) \geq n$ implies $\dim(H) = \dim(G)$ and therefore $H = G$. In this case $M = G$ has the desired properties. □

Now we can prove the theorem:

Proof. Let N denote the intersection of all $\ker \phi$ where ϕ runs through all Lie group homomorphisms from G to any nilpotent Lie group. Then N is a normal closed Lie subgroup of G and G/N is nilpotent. Moreover, if M is any normal closed Lie subgroup of G for which G/M is nilpotent, then $N \subset M$. Let $\tau : G \to G/N$ denote the natural projection.

Now prop. 1 implies:

If W is a relatively compact open subset of G, and $g_0, \ldots, g_n$ are randomly chosen elements in W, then with probability one the elements $\tau(g_i)$ do generate a dense subgroup of G/N.

On the other hand, from cor. 1 we infer:

If W is a Z-neighbourhood in G, and $g_0, \ldots, g_n$ are randomly chosen elements of W, and H is the closure of the subgroup of G generated by the g_i, then with probability one there is a normal closed Lie subgroup M of G such that G/M is nilpotent and $M \subset H$. Since G/M being nilpotent implies $N \subset M$, we obtain that $N \subset H$ with probability one.

Combined, these assertions prove the theorem: If $\tau(H)$ is dense in G/N and $N \subset H$, then H must be dense in G. □

4. Optimality

The theorem can not be improved on the number of generators for an arbitrary Lie group, since a dense subgroup of $(\mathbb{R}^d, +)$ can not be generated by less than $d+1$ elements.

The relatively compact open subset W in the statement of the theorem can be any Z-neighborhood, but not an arbitrary relatively compact open neighborhood:

Proposition 3. *Let n be a natural number and G a connected real Lie group which is not amenable.*

Then there exists a relatively compact open subset U in G such that n randomly chosen elements in U generate a non-dense subgroup with probability at least $\frac{n!}{n^n}$.

Proof. By the results of [7] we can find open subsets $V_1, \ldots, V_n$ in G such that for any choice of $g_i \in V_i$ the subgroup of G generated by the g_i is discrete (hence not dense). By shrinking the V_i we may assume that they are all relatively compact, are pairwise disjoint and have the same volume with respect to the Haar measure μ of G. Define $U = \cup_i V_i$. Observe that $\mu(V_i) = \frac{1}{n}\mu(U)$ for each i by our assumptions.

Let σ be a permutation of $\{1, \ldots, n\}$. If $g_i \in V_{\sigma(i)}$ for all $i \in \{1, \ldots, n\}$, then the subgroup generated by the g_i is discrete. For each i the probability for $g_i \in V_{\sigma(i)}$ to hold is $\frac{1}{n}$. The cardinality of all such permutations σ is $n!$. Hence with probability at least $\frac{n!}{n^n}$ randomly chosen elements $g_1, \ldots, g_n$ in U do generate a discrete (and therefore non-dense) subgroup of G. □

5. Nilpotent Lie groups

Above (see prop. 1) we proved:

Let G be a connected nilpotent Lie group and $d = \dim(G/G')$. Then there exists a subset $\Sigma \subset G^{d+1}$ of Haar measure zero such that for any $(g_1, \ldots, g_{d+1}) \in G^{d+1} \setminus \Sigma$ the subgroup generated by the g_i is dense in G.

On the other hand, in [7] we proved:

Let G be a connected nilpotent Lie group and $d = \dim(G/G')$. Then there exists a natural number $N \leq d$ such that for all $k \leq N$ there exists a subset $\Sigma_k \subset G^k$ of Haar measure zero such that for any $(g_1, \ldots, g_k) \in G^k \setminus \Sigma_k$ the subgroup generated by the g_i is discrete in G.

We would like to emphasize that it may happen that $N < d$. In this case for all $k \in \{N+1, \ldots, d\}$ any k randomly chosen elements generate a subgroup which is neither dense nor discrete (with probability one).

Example 1. *Let G be the simply-connected real nilpotent Lie group associated to the Lie algebra $\langle A, B, C, D\rangle$ with $[A, B] = C$ and $[A, C] = D$ as the only non-trivial commutator relations among the base vectors.*

G can also be described as follows: Take $\mathbb{R}^4$ as manifold and define the group law via

$$(a_1, b_1, c_1, d_1) \cdot (a_2, b_2, c_2, d_2) = \left(a_1 + a_2, b_1 + b_2, c_1 + c_2 + a_1 b_2, d_1 + d_2 + a_1 c_2 + \frac{a_1^2}{2} b_2\right)$$

Let Z be the center, i.e. $Z = \{(0, 0, 0, d) : d \in \mathbb{R}\}$ and Lie $Z = \langle D\rangle$.

Now let us chose two elements $g_i = (a_i, b_i, c_i, d_i)$ (for $i \in \{1, 2\}$). If (a_1, b_1) and (a_2, b_2) are $\mathbb{R}$-linearly independent elements of $\mathbb{R}^2$ and a_1, a_2 are $\mathbb{Q}$-linearly independent elements of $\mathbb{R}$, then the connected component of the closure of the subgroup Γ of G generated by g_1 and g_2 equals Z. In particular, in this case Γ is neither discrete nor dense.

6. Perfect Lie groups

A Lie group G is called *perfect* if it equals its own commutator group. For these special class of Lie groups better results follow immediately from the work of Breuillard and Gelander. In particular, their results imply the following:

Let G be a perfect Lie group and let k be a natural number such that the Lie algebra of G can be generated (as a Lie algebra) by k elements.

Then there is a relatively compact open neighbourhood W of e in G such that with probability one k randomly chosen elements of W will generate a dense subgroup of G.

For a semisimple Lie group this implies that 2 elements are enough (because every semisimple Lie algebra is generated by two elements),

while for an arbitrary perfect Lie group it is at least clear that $\dim G$ elements suffice.

Since our method needs $\dim G+1$ generators, the results of Breuillard and Gelander yield a better result for perfect Lie groups.

References

[1] Bourbaki, N.: Groupes et Algèbres des Lie VI/VII. Chapitres 7 et 8.

[2] Breuillard, E.; Gelander, T.: On dense free subgroups of Lie groups. *Journal of Algebra* **261**, 448-467 (2003)

[3] Dixmier, J.: Sous-algèbres de Cartan et décompositions de Levi dans les algèbres de Lie. *Trans. R. Soc. Can.* Sect. III **50**, 17–21

[4] Onishchik, A.L.; Vinberg, E.B. (Editors): Lie groups and Lie Algebras III. Encyclopedia of Mathematical Sciences. Vol. 41. Springer 1994.

[5] Raghunathan, M.S.: Discrete subgroups of Lie groups. Erg. Math. Grenzgeb. **68** , Springer (1972)

[6] Tits, J.: Free subgroups in linear groups. *J. Algebra* **20**, 250–270 (1972)

[7] Winkelmann, J.: Generic subgroups of Lie groups. *Topology*, **41** 163-181 (2002)

[8] Winkelmann, J.: On Discrete Zariski-Dense Subgroups of Algebraic Groups. *Math. Nachr.* **186**, 285–302 (1997)

[9] Zassenhaus, H.: Beweis eines Satzes über diskrete Gruppen. *Abh. Math. Sem. Hamburg* **12**, 289–312 (1938)

Jörg Winkelmann, Institut Elie Cartan (Mathématiques), Université Henri Poincaré Nancy 1, B.P. 239, F-54506 Vandœuvre-les-Nancy Cedex, France

E-mail address: jwinkel@member.ams.org

Webpage: http://www.math.unibas.ch/~winkel/